EXHIBIT A

FRANK S. HEDIN (SBN 291289)
HEDIN LLP
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Counsel for Plaintiffs and Putative Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

TERESA TURNER, individually and on behalf of all others similarly situated, Plaintiff, V. NATIONAL NOTARY ASSOCIATION, Defendant.	Case No. 2:25−cv−00334−FMO−PD **PLAINTIFF'S FIRST SET OF INTERROGATORIES**

Pursuant to Rule 33 of the Federal Rules of Civil Procedure, Plaintiff Teresa Turner requests that Defendant National Notary Association, respond to the following Interrogatories, in writing and under oath, within thirty (30) days from receipt of service.

INSTRUCTIONS[1]

1. You are required to provide all information that is available to You, including information in the possession of Your attorneys, agents, or others under Your control, and not merely information known by virtue of Your own personal knowledge.

2. If You claim any sort of privilege, whether based on statute or otherwise, as a ground for not answering, state the following:

(a) The date of any such information;

(b) The name, the present or last known home and business addresses and the telephone numbers of those individuals who prepared, produced, reproduced or were recipients of said information, or were a speaker of or listener to an oral communication;

(c) A description of the subject matter sufficient to identify it without revealing the information for which the privilege is claimed; and

(d) Each and every fact or basis upon which you claim any such privilege.

3. These Interrogatories are continuing and require supplemental responses pursuant to Federal Rule of Civil Procedure 26(e). You are obligated to change, supplement and correct Your answers to conform to all available information, including such information as becomes available to You after Your answers hereto are served.

4. If You object to any portion or aspect of any interrogatory, provide all information responsive to the portion to which You do not object.

[1] Unless otherwise defined herein, all capitalized terms shall be given the meanings assigned to them in the "Definitions" section below.

5. Where an Interrogatory asks for a date, an amount, or any other specific information, if the precise date, amount, or other specific information is unknown to You, please approximate the information requested as precisely as You are reasonably capable of doing, and indicate that You have done so.

DEFINITIONS

1. "Action" means Case No. 2:25−cv−00334 pending in the Central District of California.

2. "Facebook ID" means the unique combination of numbers associated with a user's Facebook/Meta profile.

3. "Informed Written Consent" has the meaning set forth in 18 U.S.C. § 2170(b).

4. "Meta" means the company previously known as Facebook, Inc. and now known as Meta Platforms, Inc.

5. "Person(s)" refers to natural persons, proprietorships, governmental agencies, corporations, partnerships, trusts, joint ventures, groups, associations, organizations, and all other entities.

6. "Personal Information" includes information that identifies a person as having requested or obtained specific video materials or services from You, including but not limited to a person's name, address, email address, phone number, or payment information; a person's Facebook ID; the video title, subscription, or other service requested or obtained by such person from You; the URL where such video title is accessible; or any other data value that specifies the video content or service requested or obtained by such person from You.

7. "Pixel" or "Meta Pixel" means a snippet of programming code that, once installed on a webpage, sends information to Meta.

8. "Pixel ID" refers to the number associated with Defendant's configuration of the Meta Pixel on the www.nationalnotary.org website.

9. "Plaintiff" refers to Teresa Turner, the named plaintiff in the Action.

10. "Website" means nationalnotary.org.

11."You," or "Your" refers collectively to the National Notary Association, together with all officers, directors, employees, agents, attorneys, affiliates, parents, subsidiaries, predecessors, successors, assigns, and any authorized dealers of any of the foregoing.

RULES OF CONSTRUCTION

1. The terms "all" and "each" should be construed as "all and each." The word "all" means "any and all," and the word "any" means "any and all."

2. The term "including" means "including, but not limited to." The term "include(s)" means "include(s), without limitation."

3. The connectives "and" and "or" shall be construed either disjunctively or conjunctively as necessary to bring within the scope of the discovery request all responses that might otherwise be construed to be outside of its scope.

4. The use of the singular form of any word includes the plural and vice versa.

5. The use of any tense of any verb shall also include within its meaning all other tenses of that verb.

RELEVANT TIME PERIOD

Unless otherwise stated, the relevant time period for the interrogatory is from January 13, 2023 through the present.

INTERROGATORIES

1. Identify all persons with knowledge of Your use of the Meta Pixel on Your Website.

2. State the number of Persons who requested videos, subscriptions, or other services from Your Websites and whose information was disclosed to Meta during the relevant time period.

3. Describe the time period(s) for which You have used the Meta Pixel, including the underlying events collected by the Meta Pixel and its associated parameters, on the Website.

4. State the Pixel ID(s) for the Meta Pixel(s) used on the Website.

5. Identify each individual involved in or with responsibility for the development, programming, installation or maintenance of any computer program or code on the Subject Website, including the Meta Pixel, obtained from or through any company offering digital advertising, such as targeted or custom advertising, including Meta.

6. Describe in what ways, if any, You have changed the functionality of the Meta Pixel installed on the Website, including adding, removing, or modifying categories of information, including underlying events and parameters it collects and sends or causes to be sent to Meta, along with the dates You made any changes.

7. Identify by name Your officers, employees, vendors, and agents who had actual knowledge that Your use of the Meta Pixel resulted in the disclosure of Your customers' Personal Information to Meta, at the time such disclosure was allegedly made.

8. Describe every means by which you attempted to obtain Informed Written Consent from Your customers before disclosing their Personal Information to Meta and explain when, in the sales transaction process, You attempted to obtain Informed Written Consent.

Dated: April 14, 2025

Respectfully submitted,

By: /s/ *Frank S. Hedin* .

FRANK S. HEDIN (SBN 291289)
HEDIN LLP
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Counsel for Plaintiffs and Putative Class

FRANK S. HEDIN (SBN 291289)
HEDIN LLP
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Counsel for Plaintiffs and Putative Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

TERESA TURNER, individually and on behalf of all others similarly situated, Plaintiff, V. NATIONAL NOTARY ASSOCIATION, Defendant.	Case No. 2:25−cv−00334−FMO−PD **PLAINTIFF'S FIRST SET OF REQUESTS FOR PRODUCTION**

Pursuant to Rule 34 of the Federal Rules of Civil Procedure, Plaintiff Teresa Turner requests that Defendant National Notary Association, respond to the following Requests for Production of Documents within thirty (30) days from receipt of service. The production shall occur at the offices of Hedin LLP, 1395 Brickell Ave., Suite 610, Miami, Florida, 33131, or at a location otherwise agreed upon by the parties.

INSTRUCTIONS[1]

1. In producing responsive materials, You are to furnish all documents, communications, and electronically stored information ("ESI") in Your possession, custody, or control, regardless of whether such documents, communications, or ESI are possessed directly by You or Your employees; by any agent(s) of Yours; by any of Your parent companies, subsidiaries, affiliates, or trusted business partners; by any agent(s) of any of Your parent companies, subsidiaries, affiliates, or trusted business partners; or by Your attorneys or their employees or investigators.

2. These requests are continuing and require supplemental responses pursuant to Federal Rule of Civil Procedure 26(e).

3. Production of electronically stored information should be in PDF format, and hardcopy documents should be scanned and produced as PDF images. Original document orientation shall be maintained (i.e., portrait to portrait and landscape to landscape). All documents must be searchable through Optical Character Recognition ("OCR"). When subjecting documents to an OCR process, the settings of the OCR software shall maximize text quality over process speed. Any settings such as "auto-skewing," "auto-rotation," and the like should be turned on when documents are run through the process.

4. All documents must be assigned a Bates/control number that shall always: (1) be unique across the entire document production, (2) maintain a constant length (zero/0-padded) across the entire production, (3) contain no special characters or

[1] Unless otherwise defined herein, all capitalized terms shall be given the meanings assigned to them in the "Definitions" section below.

embedded spaces, and (4) be sequential within a given document. If a Bates number or set of Bates numbers is skipped in a production, the producing party will disclose the Bates numbers or ranges in a cover letter accompanying the production.

5. Unless words or terms have been given a specific definition herein, each word or term used herein shall be given its usual and customary dictionary definition except where such words have a specific custom and usage definition in a particular trade or industry, in which case they shall be interpreted in accordance with such usual custom and usage definition of which You are aware.

DEFINITIONS

1. "Action" means Case No. 2:25−cv−00334 pending in the Central District of California.

2. "Facebook ID" means the unique combination of numbers associated with a user's Facebook/Meta profile.

3. "Informed Written Consent" has the meaning set forth in 18 U.S.C. § 2170(b).

4. "Meta" means the company previously known as Facebook, Inc. and now known as Meta Platforms, Inc.

5. "Person(s)" refers to natural persons, proprietorships, governmental agencies, corporations, partnerships, trusts, joint ventures, groups, associations, organizations, and all other entities.

6. "Personal Information" includes information that identifies a person as having requested or obtained specific video materials or services from You, including but not limited to a person's name, address, email address, phone number, or payment information; a person's Facebook ID; the video title, subscription, or other service requested or obtained by such person from You; the URL where such video title is accessible; or any other data value that specifies the video content or service requested or obtained by such person from You.

7. "Pixel" or "Meta Pixel" means a snippet of programming code that, once installed on a webpage, sends information to Meta.

8. "Pixel ID" refers to the number associated with Defendant's configuration of the Meta Pixel on the www.nationalnotary.org website.

9. "Plaintiff" refers to Teresa Turner, the named plaintiff in the Action.

10. "Website" means nationalnotary.org.

11. "You," or "Your" refers collectively to National Notary Association, together with all officers, directors, employees, agents, attorneys, affiliates, parents, subsidiaries, predecessors, successors, assigns, and any authorized dealers of any of the foregoing.

RULES OF CONSTRUCTION

1. The terms "all" and "each" should be construed as "all and each." The word "all" means "any and all," and the word "any" means "any and all."

2. The term "including" means "including but not limited to." The term "include(s)" means "include(s), without limitation."

3. The connectives "and" and "or" shall be construed either disjunctively or conjunctively as necessary to bring within the scope of the discovery request all responses that might otherwise be construed to be outside of its scope.

4. The use of the singular form of any word includes the plural and vice versa.

5. The use of any tense of any verb shall also include within its meaning all other tenses of that verb.

RELEVANT TIME PERIOD

Unless otherwise stated, the relevant time period for the production is from January 13, 2023 through the present.

DOCUMENTS TO BE PRODUCED

1. All documents, communications and ESI concerning the Plaintiff.

2. All documents, communications, and ESI concerning Your transmission of any Person's Personal Information to Meta.

3. All contracts, agreements, statements of work, work orders, order forms, or the like exchanged between You (or any other party acting on Your behalf) and Meta concerning Your use of the Metal Pixel or Your transmission of Personal Information to Meta.

4. All documents, communications, and ESI concerning the Meta Pixel, including the use of the Meta Pixel on Your website, Your Pixel ID, the ranges of dates during which the Meta Pixel was in use on the Website, and the conditions under which the Meta Pixel and its underlying events and parameters shared (or caused the sharing of) Personal Information of Your Website users with Meta.

5. All documents, communications, and ESI concerning Your decision to implement, and the installation of, the Meta Pixel, and its underlying events and parameters, on Your Website.

6. Documents, communications, and ESI, showing all the Personal Information that was shared with Meta via the Meta Pixel on Your Website.

7. All documents, communications, and ESI concerning the effect that Your use of the Meta Pixel, including Your transmission of Personal Information to Meta, has had on Your revenues, profits, projections or customer numbers.

8. Website code, technical documentation, technical papers, and computer source code sufficient to show the manner in which Your Website operated to collect and transmit Your customers' Personal Information by or through the Meta Pixel and its underlying events and parameters installed on Your website.

9. All documents, communications, and ESI concerning inquiries, comments or complaints received by You concerning the sharing of customer information with Meta.

10. All documents, communications, and ESI regarding this Action or any other lawsuit or contemplated lawsuit alleging violations of the VPPA arising out of the use of the Meta Pixel, excluding privileged communications between You and Your counsel.

11. Documents, communications, and ESI sufficient to show the number of unique Persons who requested or obtained any videos, subscriptions, or other services from Your Website, as well as documents, communications, and ESI sufficient to show the total number of purchases of and requests for videos, subscriptions, or other services on Your Website.

12. All documents, communications, and ESI sufficient to identify all the Persons who requested or obtained video materials or other services from You and whose Personal Information was transmitted to Meta, specifically including those individuals' names and email addresses.

13. All documents, communications and ESI that You contend evidence the Informed Written Consent of the Plaintiff, or of any other Person who purchased or otherwise requested or obtained video materials or services from You, to transmit or otherwise disclose such Person's Personal Information to Meta.

14. Organizational charts and similar documents, communications, and ESI identifying Your affiliates, subsidiaries, or parents, as well as lists of the directors, officers, employees (and their titles or job positions) of You and each of Your affiliates, subsidiaries, or parents.

15. All documents, communications, and ESI concerning any insurance agreement under which any Person carrying on an insurance business may be liable to satisfy part or all of a judgment which may be entered in this Action or to indemnify or reimburse You for payments made to satisfy any such judgment.

16. Documents sufficient to show Your document retention policies, including document retention or destruction policies with respect to e-mail or other electronically stored or recorded documents.

17. All documents, communications, and ESI identified, referenced, or contemplated in Your answers to Plaintiff's Interrogatories, or otherwise relied upon in answering Plaintiff's Interrogatories.

18. All documents, communications, and ESI that You intend to use to support any affirmative defense to Plaintiff's claims alleged in the Action.

19. All documents, communications, and ESI that You intend to use to contest or oppose the certification of a class in the Action.

Dated: April 14, 2025

Respectfully submitted,

By: /s/ *Frank S. Hedin* .

FRANK S. HEDIN (SBN 291289)
HEDIN LLP
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Counsel for Plaintiffs and Putative Class

HEDIN LLP

1395 Brickell Avenue, Suite 610
Miami, Florida 33131-3353
www.hedinllp.com

Elliot O. Jackson
(305) 357-2107
ejackson@hedinllp.com

April 14, 2025

VIA EMAIL

Myriah V. Jaworski
Chirag Patel
CLARK HILL LLP
600 W. Broadway Suite 500
San Diego, California 92101

Re: *Turner v. National Notary Association*, No. 2:25-cv-00334-FMO-PD (C.D. Cal.)

Dear Counsel:

Please take notice that pursuant to Federal Rule of Civil Procedure 45, Plaintiff, in the aforementioned matter, will request that Meta Platforms, Inc. ("Meta") and Momentive Software, Inc. d/b/a CrowdWisdom produce documents. True and correct copies of the subpoenas that will be served are enclosed with this correspondence.

Sincerely,

Elliot O. Jackson

Cc: all counsel of record (via email)

AO 88B (Rev. 02/14) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action

UNITED STATES DISTRICT COURT

for the

Central District of California

Teresa Turner

Plaintiff

v.

National Notary Association

Defendant

Civil Action No. 2:25-cv-00334-FMO-PD

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: Meta Platforms, Inc.
1 Meta Way, Menlo Park, CA 94025

(Name of person to whom this subpoena is directed)

☑ *Production:* **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material: See Schedule A

Place:	Date and Time:
HEDIN LLP 535 Mission Street, 14th Floor San Francisco, CA 94105	April 30, 2025 at 10:00 AM

☐ *Inspection of Premises:* **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 04/14/2025

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

/s/ Elliot O. Jackson

Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Teresa Turner, who issues or requests this subpoena, are:

Elliot O. Jackson, 1395 Brickell Ave. Suite 610 Miami, Florida 33131, ejackson@hedinllp.com, 305-357-2107

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 2:25-cv-00334-FMO-PD

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named person as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Print Save As... Add Attachment Reset

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

SCHEDULE A

DEFINITIONS

1. "Action" refers to *Turner v. National Notary Association*, Case No. 2:25-cv-00334-FMO-PD pending in the Central District of California. A copy of the operative pleading is attached hereto as **Exhibit 1**.

2. "Communications" means any disclosure, transfer, or exchange of information or opinion, however made.

3. "Concerning" means comprising, consisting, containing, setting forth, showing, disclosing, describing, explaining, mentioning, evidencing, reflecting, embodying, summarizing, relating to, or referring to, directly or indirectly.

4. "Defendant" refers to the National Notary Association (Pixel ID: 184234421926479).

5. "Documents" is defined to be synonymous in meaning and equal in scope to the usage of this term in Federal Rule of Civil Procedure 34(a), and includes Electronically Stored Information ("ESI").

6. "Facebook" means the Facebook social media platform.

7. "Facebook ID" means the unique combination of numbers associated with a user's Facebook profile.

8. "Identify" means (a) to state a person's full name, home address, business address, and present and past relationship to any party; or (b) to state the title of any document, who prepared it, when it was prepared, where it is located, and who its custodian is.

9. "Meta" means Meta Platforms, Inc., formerly known as Facebook, Inc., and includes all predecessors, successors, divisions, subsidiaries, and affiliates, and any agents, consultants, or other persons acting for or on behalf of any of them.

10. "Personally Identifiable Information" means information that identifies a person as having requested or obtained specific video materials or services from a video tape service provider, and is synonymous in meaning and equal in scope to the usage of this term in 18 U.S.C. § 2710(a)(3). For the purposes of these requests, Defendant is a "video tape service provider."

11. "Pixel" or "Pixels" means programming code that, once installed on a website, sends information about the Website's subscribers or users to Meta.

12. "Pixel ID" refers to the number associated with Defendant's website, which is 184234421926479.

13. "Plaintiff" refers to the named plaintiff in the Action, Teresa Turner, whose FID is 100000451901971.

14. "VPPA" means the Video Privacy Protection Act, 18 U.S.C. § 2710.

15. "Website" means www.nationalnotary.org.

16. "You" and "Your" as used herein shall refer to Meta and any of its parents, predecessors, other affiliates, successors, or subsidiaries, including officers, directors, employees, partners, agents, consultants, or any other person acting or purporting to act on behalf of such entities.

INSTRUCTIONS

1. Unless otherwise specified, the relevant time period for purposes of these requests is from January 13, 2023 through the date of Your responses and includes all documents and

information relating to events or transactions within this period, even if prepared, received, or reviewed outside of this period.

2. Documents shall be produced in the manner and order in which they appear in Your files, and shall not be shuffled or otherwise rearranged. Documents that were, in their original condition, stapled, clipped, or otherwise fastened together shall be produced in such form.

3. For any objection grounded on a privilege or immunity, set forth the facts and supporting material, including, where necessary, a privilege log disclosing the general nature of what is being withheld and substantiating the basis of any claim of privilege or immunity, including:

a. The name(s) of the author(s) of the document;
b. The name(s) of the sender(s) of the document;
c. The name(s) of the person(s) who received the document or to whom copies were sent or exhibited at any time;
d. The name(s) of all persons presently having possession of the document or a copy thereof;
e. A brief description of the nature and subject matter of the document; and
f. The privilege asserted and the statute, rule, decision, or other basis that is claimed to give rise to the privilege.

4. If no documents exist that are responsive to any request to identify or to produce, so state.

DOCUMENT REQUESTS

1. All Documents concerning Plaintiff (FID: 100000451901971) and Defendant (Pixel ID: 184234421926479), including any video materials Plaintiff requested or obtained from the Website, the Website URLs she visited, or any other information Concerning Plaintiff, Defendant, and the Website in Meta's custody, possession, or control.

2. Without temporal restriction, all Documents concerning the creation and installation of any Pixels on the Website, including all Documents, Communications, and other

information concerning the creation of the account, online agreement, and/or online dashboard configurations.

3. Without temporal restriction, all Communications between Meta and Defendant relating to any Pixel embedded on the Website, including Communications describing what information would be or has been transmitted to Meta by Defendant or via the Pixels embedded on the Website.

4. Without temporal restriction, Documents sufficient to indicate the period of time that Meta has received information via any Pixel embedded on the Website.

5. Without temporal restriction, Documents sufficient to Identify how the Meta Pixel was set up, configured, and implemented for the Website and/or Defendant.

6. Documents sufficient to show transmissions of data or information from the Website and/or Defendant to Meta via the Pixel embedded on the Website that include: (i) a Meta user's Facebook ID; (ii) the titles of any prerecorded video materials requested, purchased, or obtained by the Meta user; (iii) the URL of any prerecorded video materials requested, purchased, or obtained by the Meta user; and/or (iv) any other data or information that provides the title of the prerecorded video materials the Meta user requested, purchased, or obtained.

7. Without temporal restriction, Documents sufficient to show all discrete types or categories of information or events that the Website and/or Defendant transmit, or has or have transmitted, to Meta via the Pixel.

8. Documents sufficient to Identify all Personally Identifiable Information disclosed to Meta through the Pixel by the Website and/or Defendant.

9. Documents sufficient to show the number of Meta users for whom the following information was transmitted to Meta from the Website via the Pixel: (i) their Facebook IDs; (ii)

the titles of any prerecorded video materials or subscriptions accessed, viewed, requested, purchased, or obtained by the Meta user; (iii) the URL of any prerecorded video materials accessed, viewed, requested or obtained by the Meta user; (iv) the URLs of any pages accessed, viewed, requested, or obtained by the Meta user; (v) and/or any other data or information that provides the title of the prerecorded video materials the Meta user requested or obtained.

10. Documents sufficient to show each transmission to Meta from the Website and/or Defendant via the Pixel that included one of Meta's user's: (i) Facebook IDs; (ii) the titles of any prerecorded video materials or subscriptions requested, purchased or obtained by the Meta user; the URL of any prerecorded video materials accessed, viewed, requested, purchased, or obtained by the Meta user; (iv) the URLs of any pages accessed, viewed, requested, purchased, or obtained by the Meta user; (v) and/or any other data or information that provides the title of the prerecorded video materials the Meta user requested, purchased, or obtained.

11. Documents sufficient to Identify each person whose Personally Identifiable Information was disclosed to Meta by the Website and/or Defendant through the Pixel.

12. Documents sufficient to demonstrate all purposes for which Meta uses or used data or information transmitted via the Pixel from the Website and/or Defendant.

13. All Documents and Communications relating to this Action, including Communications between Meta and Defendant, non-privileged Documents and Communications internal to Meta, and non-privileged Communications between Meta and any other third party.

14. All Communications between Meta and Defendant relating to Plaintiff's Facebook account.

EXHIBIT 1

Frank S. Hedin (SBN 291289)
Hedin LLP
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Counsel for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

TERESA TURNER, individually and on behalf of all others similarly situated, Plaintiff, V. NATIONAL NOTARY ASSOCIATION, Defendant.	Case No. 2:25-cv-334 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Teresa Turner, individually and on behalf of all others similarly situated, makes the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to herself or her counsel, which are based on personal knowledge.

A. NATURE OF THE CASE

1. Plaintiff brings this action to redress Defendant's practice of selling, renting, transmitting, and/or otherwise disclosing to Meta, records containing the

personal information of each of its customers, along with detailed information revealing the titles and subject matter of the videos and other audiovisual materials purchased by each customer in violation of the Video Privacy Protection Act, 18 U.S.C. § 2710 et seq. ("VPPA").

2. Over the past two years, Defendant has systematically transmitted (and continue to transmit today) its customers' personally identifying video viewing information to third parties, such as Meta Platforms, Inc. ("Meta"). The programming code for Meta is called the "Meta Pixel," which Defendant chose to install on the www.nationalnotary.org website.

3. The information Defendant disclosed (and continues to disclose) to Meta via the Meta Pixel includes the customer's Facebook ID ("FID") and the specific title of prerecorded videos that each of its customers purchased on Defendant's Website. An FID is a unique sequence of numbers linked to a specific Meta profile. A Meta profile, in turn, identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person). Entering "Facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name, but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta

information that reveals a particular person purchased a specific title of a prerecorded video on Defendant's Website (hereinafter, "Private Video Information").

4. Defendant disclosed and continue to disclose its customers' Private Video Information to Meta without asking for, let alone obtaining, their consent to these practices.

5. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), damages in the amount of $2,500.00, *see id.* § 2710(c).

6. Accordingly, on behalf of herself and the putative Class members defined below, Plaintiff brings this Class Action Complaint against Defendant for intentionally and unlawfully disclosing her and Putative Class members' Private Video Information to Meta.

B. PARTIES

I. Plaintiff Teresa Turner

7. Plaintiff is, and at all times relevant hereto was, a citizen and resident of San Luis Obispo County, California.

8. Plaintiff is, and at all times relevant hereto was, a user of Meta.

9. Plaintiff is a consumer of the video products and services offered on Defendant's www.nationalnotary.org website. Including on or about August 2024, Plaintiff purchased prerecorded video material from Defendant's www.nationalnotary.org website by requesting and paying for such material, providing her name, email address, and home address for delivery of such material. Defendant completed the sales of goods to Plaintiff by shipping or delivering the prerecorded video material she purchased to the address she provided in her order. Accordingly, Plaintiff requested or obtained, and is therefore a consumer of, prerecorded video material sold by Defendant on its website.

10. At all times relevant hereto, including when requesting or obtaining prerecorded video material from Defendant's website, Plaintiff had a Meta account, a Meta profile displaying her name and picture, and an FID associated with such profile.

11. Plaintiff has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Private Video Information to Meta. In fact, Defendant has never even provided Plaintiff with written notice of its practices of disclosing its customers' Private Video Information to third parties such as Meta.

12. Prior to and at the time she purchased prerecorded video material from Defendant, Defendant did not notify Plaintiff that it would disclose the Private Video Information of its customers generally or that of Plaintiff in particular, and Plaintiff has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her

Private Video Information to third parties. Plaintiff has never been provided any written notice that Defendant discloses its customers' Private Video Information or any means of opting out of such disclosures of her Private Video Information.

13. Because Defendant disclosed Plaintiff's Private Video Information (including her FID, unique identifiers, and her request or purchase of prerecorded video material from Defendant's website) to third parties during the applicable statutory period, Defendant violated Plaintiff's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

II. Defendant

14. Defendant National Notary Association is a not-for-profit corporation organized under the laws of California, with its headquarters at 9350 De Soto Ave., Chatsworth, California 91311. Defendant is the largest and oldest organization in the United States serving notaries and training persons to be notaries through certifications, trainings, seminars, conferences, and printed and online educational materials that accompany these programs.

C. JURISDICTION AND VENUE

15. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

16. Personal jurisdiction and venue are proper because Defendant maintains its headquarters and principal place of business in Los Angeles, California, within this judicial District.

VIDEO PRIVACY PROTECTION ACT

17. The VPPA prohibits companies (like Defendant) from knowingly disclosing to third parties (like Meta) information that personally identifies consumers (like Plaintiff) as having requested or obtained specific video(s) or other audio-visual materials from its Website.

18. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4). It defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

19. Leading up to the VPPA's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

20. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, the personal nature of such information, and the need to protect it from disclosure, is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id.*

21. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a more recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[1]

22. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[2]

23. In this case, however, Defendant deprived Plaintiff and numerous other similarly situated persons of that right by systematically (and surreptitiously)

---

[1] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary. senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the- 21stcentury.

[2] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, franken.senate.gov (Jan. 31, 2012).

disclosing their Private Video Information to Meta, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

24. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[3]

25. Over two decades later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a 26 billion dollar per year online advertising industry in the United States.[4]

26. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

[3] Transcript, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[4] *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), available at https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[5]

27. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[6]

28. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[7]

---

[5] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

[6] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), available at http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/ .

[7] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), available at https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html#:~:text=It's%20called%20the%20Acxiom%20Corporation,to%20know%20much%2C%20much%20more.

29. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[8]

30. Recognizing the severe threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[9]

31. Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers

---

[8] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. On Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) available at https://www.commerce.senate.gov/services/files/3bb94703-5ac8-4157-a97b-%20a658c3c3061c.

[9] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012), available at https://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like Defendant share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the "[v]ast databases" of consumer data that are often "sold to thieves by large publicly traded companies," which "put[s] almost anyone within the reach of fraudulent telemarketers" and other criminals.[10]

32. Disclosures like Defendant's are particularly dangerous to the elderly. "Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide."[11]

33. The FTC notes that "[t]he elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers."[12]

34. Indeed, an entire black market exists while the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like

---

[10] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at https://www.nytimes.com/2007/05/20/business/20tele.html.

[11] *Id*.

[12] Prepared Statement of the FTC on "Fraud Against Seniors" before the Special Committee on Aging, United States Senate (August 10, 2000).

Defendant's are particularly troublesome because of their cascading nature: "Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[13]

35. Defendant is not alone in violating its customers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

II. Consumers Place Monetary Value on Their Privacy and Consider Privacy Practices When Making Purchases

36. As the data aggregation industry has grown, so has consumer concerns regarding personal information.

37. A survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do protect their privacy online.[14] As a result, 81 percent of smartphone

[13] *Id*.

[14] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[15]

38. Thus, as consumer privacy concerns grow, consumers increasingly incorporate privacy concerns and values into their purchasing decisions, and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[16]

39. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[17]

---

[15] *Id*.

[16] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), available at https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

[17] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on Monetizing Privacy*

40. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[18] As such, where a business offers customers a product or service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a product or service of less value than the product or service paid for.

III. Defendant Use the Meta Pixel to Systematically Disclose its customers' Private Video Information to Meta

41. As alleged below, when a consumer requests or obtains a particular prerecorded video on Defendant's Website, the Meta Pixel technology that Defendant intentionally installed on its Website transmits (1) the unencrypted FID for each purchaser; (2) detailed information revealing the titles and subject matter of the prerecorded videos requested or obtained by each of its purchasers; and (3) the URL where such videos are available for purchase, without the consumer's consent and in clear violation of the VPPA.

(Feb. 27, 2012), available at https://www.enisa.europa.eu/publications/monetising-privacy.

[18] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf.

A. The Meta Pixel

42. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta".[19] Meta is now the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birth date, gender, and phone number or email address.

43. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to monitor and track the actions taken by visitors to their websites and to report them back to Meta. This allows companies like Defendant to build detailed profiles about its customers and to serve them with highly targeted advertising.

44. Additionally, the Meta Pixel installed on a company's website allows Meta to "match [] website visitors to their respective Facebook User accounts."[20] This is because Meta has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name[21] – and because each transmission of information made

[19] *See* Facebook, "Company Info," available at https://about.fb.com/company-info./.

[20] Meta, "Get Started – Meta Pixel," available at https://developers.facebook.com/docs/meta-pixel/get-started/.

[21] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark

from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor.

45. As Meta's developer's guide explains, installing the Meta Pixel on a website allows Meta to track actions that users with Meta accounts take on the site. Meta states that "Examples of [these] actions include adding an item to their shopping cart or making a purchase."[22]

46. Meta's Business Tools Terms govern the use of Meta's Business Tools, including the Meta Pixel.[23]

47. Meta's Business Tools Terms state that website operators may use Meta's Business Tools, including the Meta Pixel, to transmit the "Contact Information" and "Event Data" of their website's visitors to Meta.

48. Meta's Business Tools Terms define "Contact Information" as "information that personally identifies individuals, such as names, email addresses, and phone numbers . . . ."[24]

Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

[22] Meta, "About Meta Pixel," available at https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[23] Meta, "Meta Business Tools Terms," available at https://www.facebook.com/legal/technology_terms.

[24] *Id.*

49. Meta's Business Tools Terms state: "You instruct us to process the Contact Information solely to match the Contact Information against user IDs [e.g., FIDs] ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data."[25]

50. The Business Tools Terms define "Event Data" as, *inter alia*, "information that you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps, and purchases of your products."[26]

51. Website operators use the Meta Pixel to send information about visitors to their Websites to Meta. Every transmission to Meta accomplished through the Meta Pixel includes at least two elements: (1) the website visitor's FID and (2) the webpage's URL triggering the transmission.

52. Depending on the configuration of the Meta Pixel, the website may also send Event Data to Meta. Defendant have configured the Meta Pixel on its Website to send Event Data to Meta.

[25] *Id.*

[26] *Id.*

53. When website operators make transmissions to Meta through the Meta Pixel, none of the following categories of information are hashed or encrypted: the visitor's FID, the website URL, or the Event Data.

54. Every website operator installing the Meta Pixel must agree to the Meta Business Tools Terms.[27]

55. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after the consumer's browser history has been cleared.

56. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

57. Simply put, if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it

[27] *See id.*

transmits) are then able to "track [] the people and type of actions they take,"[28] including, as relevant here, the specific prerecorded video material that they purchase from Defendant's website.

B. Defendant Knowingly Uses the Meta Pixel to Transmit the Private Video Information of its Customers to Meta

58. Defendant sells various prerecorded video materials on its Website, www.nationalnotary.org, including online courses and certification programs on various topics, including becoming a licensed notary or signing agent.

59. To purchase prerecorded video material from both Defendant's Website, a person must provide at least his or her name, email address, billing address, and credit or debit card (or other form of payment) information.

60. During the purchase process on Defendant's Website, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the person who made the purchase and the specific title of video material that the person purchased (as well as the URL where such video material is available for purchase).

[28] Meta, "Retargeting: How to Advertise to Existing Customers with Ads on Facebook," available at https://www.facebook.com/business/goals/retargeting?checkpoint_src=any.

61. In order to take advantage of the targeted advertising and other informational and analytical services offered by Meta, Defendant intentionally programmed its Website (by following step-by-step instructions from Meta's website) to include the Meta Pixel code, which systematically transmits to Meta the FID of each person with a Meta account who purchases prerecorded video material on Defendant's Website, along with the specific title of the prerecorded video material that the person purchased.

62. With only a person's FID and the title of the prerecorded video material (or URL where such material is available for purchase) that the person purchased from Defendant's Website —all of which Defendant knowingly and systematically provides to Meta—any ordinary person could learn the identity of the person to whom the FID corresponds and the subscription or the title of the specific prerecorded video material that the person purchased (and thus requested and obtained). This can be accomplished simply by accessing the URL www.facebook.com/ and inserting the person's FID.

63. Defendant's practice of disclosing the Private Video Information of its customers to Meta continued unabated for the duration of the two-year period preceding the filing of this action. At all times relevant hereto, whenever Plaintiff or any other person purchased prerecorded video material from Defendant on its Website, Defendant disclosed to Meta (*inter alia*) the specific title of the video material that was requested or obtained (including the URL where such material is available for

purchase), along with the FID of the person who requested or obtained it (which, as discussed above, uniquely identified the person).

64. At all times relevant hereto, Defendant knew the Meta Pixel was disclosing its customers' Private Video Information to Meta.

65. Although Defendant could easily have programmed its Website so that none of its customers' Private Video Information is disclosed to Meta, Defendant instead chose to program its Website so that all of its customers' Private Video Information is disclosed to Meta.

66. Before transmitting its customers' Private Video Information to Meta, Defendant failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

67. By intentionally disclosing to Meta Plaintiff's and their other customers' FIDs together with the specific title of the prerecorded video material that they each purchased, without any of their consent to these practices, Defendant knowingly violated the VPPA on an enormous scale.

CLASS ACTION ALLEGATIONS

68. Plaintiff seeks to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, purchased prerecorded video material or services from Defendant's Website while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

69. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the Defendant's membership records.

70. Common questions of law and fact exist for all Class members and predominate over questions affecting only individual class members. Common legal and factual questions include but are not limited to (a) whether Defendant embedded Meta Pixel on its Website that monitors and tracks actions taken by visitors to its Website; (b) whether Defendant reports the actions and information of visitors to Meta; (c) whether Defendant knowingly disclosed Plaintiff's and Class members' Private Video Information to Meta; (d) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; and (e) whether Plaintiff and Class members are entitled to a statutory damage award of $2,500, as provided by the VPPA.

71. The named Plaintiff's claims are typical of the claims of the Class in that the Defendant's conduct toward the putative class is the same. That is, Defendant embedded the Meta Pixel on its Website to monitor and track actions taken by consumers on its Website and report this to Meta. Further, the named Plaintiff and the Class members suffered invasions of their statutorily protected right to privacy (as

afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Private Purchase Information to Meta.

72. Plaintiff is an adequate representative of the Class because she is interested in the litigation; her interests do not conflict with those of the Class members she seeks to represent; she has retained competent counsel experienced in prosecuting class actions; and she intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of all Class members.

73. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication of the common questions of law and fact, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability

issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION
Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710

74. Plaintiff repeats the allegations asserted in the preceding paragraphs as if fully set forth herein.

75. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

76. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant are each a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because they engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

77. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiff and Class members are each a "consumer" within the meaning

of the VPPA because they each purchased prerecorded video material or services from Defendant's Website that were sold and delivered to them by Defendant.

78. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The Private Video Information that Defendant transmitted to Meta constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because it identified Plaintiff and Class members to Meta as an individual who "requested or obtained," specific prerecorded video material from Defendant's Website.

79. Defendant knowingly disclosed Plaintiff's and Class members' Private Video Information to Meta via the Meta Pixel technology because Defendant intentionally installed and programmed the Meta Pixel code on its Website, knowing that such code would transmit the prerecorded video material requested or obtained by their consumers and the consumers' unique identifiers (including FIDs).

80. Defendant failed to obtain informed written consent from Plaintiff or Class members authorizing Defendant to disclose their Private Video Information to Meta or any other third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who requested or obtained prerecorded video material or services on Defendant's Website (including Plaintiff or Class members) informed, written consent that was given in a form distinct

and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

81. By disclosing Plaintiff's and Class members' Private Video Information, Defendant violated their statutorily protected right to privacy in their Private Video Information.

82. Consequently, Defendant is liable to Plaintiff and Class members for damages in the statutorily set sum of $2,500. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendant as follows:

a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as the representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b) For an order declaring that Defendant's conduct as described herein violated the VPPA;

c) For an order finding in favor of Plaintiff and the Class and against Defendant on all counts asserted herein;

d) For an award of $2,500.00 to Plaintiff and each Class member, as provided by 18 U.S.C. § 2710(c);

e) For an order permanently enjoining Defendant from disclosing the Private Video Information of its subscribers to third parties in violation of the VPPA;

f) For prejudgment interest on all amounts awarded; and

g) For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiff and the Class under Rule 23 and 18 U.S.C. § 2710(c).

Dated: January 13, 2025

Respectfully submitted,

HEDIN LLP

By: /s/ *Frank S. Hedin*

FRANK S. HEDIN (SBN 291289)
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Counsel for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

for the

Central District of California

Teresa Turner

Plaintiff

v.

National Notary Association

Defendant

Civil Action No. 2:25-cv-00334-FMO-PD

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: Momentive Software, Inc.
9620 Executive Center Dr. N #200 St. Petersburg, FL 33702

(Name of person to whom this subpoena is directed)

☑ *Production:* **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material: See Schedule A

Place:	Date and Time:
HEDIN LLP 535 Mission Street, 14th Floor San Francisco, CA 94105	April 30, 2025 at 10:00 AM

☐ *Inspection of Premises:* **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 04/14/2025

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

/s/ Elliot O. Jackson

Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Teresa Turner, who issues or requests this subpoena, are:

Elliot O. Jackson, 1395 Brickell Ave. Suite 610 Miami, Florida 33131, ejackson@hedinllp.com, 305-357-2107

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 2:25-cv-00334-FMO-PD

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named person as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Print Save As... Add Attachment Reset

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

SCHEDULE A

DEFINITIONS

1. "Action" refers to *Turner v. National Notary Association*, Case No. 2:25-cv-00334-FMO-PD pending in the Central District of California. A copy of the operative pleading is attached hereto as **Exhibit 1**.

2. "Communications" means any disclosure, transfer, or exchange of information or opinion, however made.

3. "Concerning" means comprising, consisting, containing, setting forth, showing, disclosing, describing, explaining, mentioning, evidencing, reflecting, embodying, summarizing, relating to, or referring to, directly or indirectly.

4. "CrowdWisdom" refers to the learning management system and external platform that Defendant uses to host prerecorded video courses.

5. "Defendant" refers to the National Notary Association.

6. "Documents" is defined to be synonymous in meaning and equal in scope to the usage of this term in Federal Rule of Civil Procedure 34(a), and includes Electronically Stored Information ("ESI").

7. "Facebook" means the Facebook social media platform.

8. "Identify" means (a) to state a person's full name, home address, business address, and present and past relationship to any party; or (b) to state the title of any document, who prepared it, when it was prepared, where it is located, and who its custodian is.

9. "Meta" means Meta Platforms, Inc., formerly known as Facebook, Inc., and includes all predecessors, successors, divisions, subsidiaries, and affiliates, and any agents, consultants, or other persons acting for or on behalf of any of them.

10. "Personally Identifiable Information" means information that identifies a person as having requested or obtained specific video materials or services from a video tape service provider, and is synonymous in meaning and equal in scope to the usage of this term in 18 U.S.C. § 2710(a)(3). For the purposes of these requests, Defendant is a "video tape service provider."

11. "Pixel" or "Pixels" means programming code that, once installed on a website, sends information about the Website's subscribers or users to Meta.

12. "Plaintiff" refers to the named plaintiff in the Action, Teresa Turner.

13. "VPPA" means the Video Privacy Protection Act, 18 U.S.C. § 2710.

14. "Website" means www.nationalnotary.org.

15. "You" and "Your" as used herein shall refer to Momentive Software, Inc. and any of its parents, predecessors, other affiliates, successors, or subsidiaries, including officers, directors, employees, partners, agents, consultants, or any other person acting or purporting to act on behalf of such entities.

INSTRUCTIONS

1. Unless otherwise specified, the relevant time period for purposes of these requests is from January 13, 2023, through the date of Your responses and includes all documents and information relating to events or transactions within this period, even if prepared, received, or reviewed outside of this period.

2. Documents shall be produced in the manner and order in which they appear in Your files, and shall not be shuffled or otherwise rearranged. Documents that were, in their original condition, stapled, clipped, or otherwise fastened together shall be produced in such form.

3. For any objection grounded on a privilege or immunity, set forth the facts and supporting material, including, where necessary, a privilege log disclosing the general nature of

what is being withheld and substantiating the basis of any claim of privilege or immunity, including:

a. The name(s) of the author(s) of the document;
b. The name(s) of the sender(s) of the document;
c. The name(s) of the person(s) who received the document or to whom copies were sent or exhibited at any time;
d. The name(s) of all persons presently having possession of the document or a copy thereof;
e. A brief description of the nature and subject matter of the document; and
f. The privilege asserted and the statute, rule, decision, or other basis that is claimed to give rise to the privilege.

4. If no documents exist that are responsive to any request to identify or to produce, so state.

DOCUMENT REQUESTS

1. All Documents concerning Plaintiff and Defendant, including any video materials Plaintiff requested or obtained from the Website, the Website URLs she visited, or any other information Concerning Plaintiff, Defendant, and the Website in Your custody, possession, or control.

2. Without temporal restriction, all Documents concerning the Defendant's purchase, selection, installation, and configuration of the CrowdWisdom platform on the Website, including all Documents, Communications, and other information concerning the creation of the account, online agreement, and/or online dashboard configurations.

3. Without temporal restriction, all Communications between You or CrowdWisdom and Defendant relating to any purchases made on the Website, including Communications describing what information would be or has been transmitted to You or CrowdWisdom by Defendant or via the Pixels embedded on the Website.

4. Without temporal restriction, Documents sufficient to indicate the period of time that You or CrowdWisdom has received information from the Website.

5. Without temporal restriction, Documents sufficient to Identify how the CrowdWisdom system was set up, configured, and implemented for the Website and/or Defendant.

6. Documents sufficient to show transmissions of data or information from the Website and/or Defendant to You or CrowdWisdom.

7. Without temporal restriction, Documents sufficient to show all discrete types or categories of information or events that the Website and/or Defendant transmit, or has or have transmitted, to You or CrowdWisdom.

8. Documents sufficient to Identify all Personally Identifiable Information disclosed to You or CrowdWisdom by the Website and/or Defendant.

9. Documents sufficient to show the number of purchasers from Defendant's Website for whom the following information was transmitted to You or CrowdWisdom: (i) the titles of any prerecorded video materials or subscriptions accessed, viewed, requested, purchased, or obtained by the Meta user; (ii) the URL of any prerecorded video materials accessed, viewed, requested or obtained by the user; (iv) the URLs of any pages accessed, viewed, requested, or obtained by the user; (v) and/or any other data or information that provides the title of the prerecorded video materials the Meta user requested or obtained.

10. Documents sufficient to Identify each person whose Personally Identifiable Information was disclosed to You or CrowdWisdom by the Website and/or Defendant.

11. Documents sufficient to demonstrate all purposes for which You or CrowdWisdom uses or used data or information transmitted by the Website and/or Defendant.

12. All Documents and Communications relating to this Action, including Communications between You or CrowdWisdom and Defendant, non-privileged Documents and

Communications internal to You or CrowdWisdom, and non-privileged Communications between You or CrowdWisdom and any other third party.

13. Any and all contracts and indemnification agreements between You and Defendant.

EXHIBIT 1

Frank S. Hedin (SBN 291289)
Hedin LLP
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Counsel for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

TERESA TURNER, individually and on behalf of all others similarly situated, Plaintiff, V. NATIONAL NOTARY ASSOCIATION, Defendant.	Case No. 2:25-cv-334 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Teresa Turner, individually and on behalf of all others similarly situated, makes the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to herself or her counsel, which are based on personal knowledge.

A. NATURE OF THE CASE

1. Plaintiff brings this action to redress Defendant's practice of selling, renting, transmitting, and/or otherwise disclosing to Meta, records containing the

personal information of each of its customers, along with detailed information revealing the titles and subject matter of the videos and other audiovisual materials purchased by each customer in violation of the Video Privacy Protection Act, 18 U.S.C. § 2710 et seq. ("VPPA").

2. Over the past two years, Defendant has systematically transmitted (and continue to transmit today) its customers' personally identifying video viewing information to third parties, such as Meta Platforms, Inc. ("Meta"). The programming code for Meta is called the "Meta Pixel," which Defendant chose to install on the www.nationalnotary.org website.

3. The information Defendant disclosed (and continues to disclose) to Meta via the Meta Pixel includes the customer's Facebook ID ("FID") and the specific title of prerecorded videos that each of its customers purchased on Defendant's Website. An FID is a unique sequence of numbers linked to a specific Meta profile. A Meta profile, in turn, identifies by name the specific person to whom the profile belongs (and also contains other personally identifying information about the person). Entering "Facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name, but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta

information that reveals a particular person purchased a specific title of a prerecorded video on Defendant's Website (hereinafter, "Private Video Information").

4. Defendant disclosed and continue to disclose its customers' Private Video Information to Meta without asking for, let alone obtaining, their consent to these practices.

5. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), damages in the amount of $2,500.00, *see id.* § 2710(c).

6. Accordingly, on behalf of herself and the putative Class members defined below, Plaintiff brings this Class Action Complaint against Defendant for intentionally and unlawfully disclosing her and Putative Class members' Private Video Information to Meta.

B. PARTIES

I. Plaintiff Teresa Turner

7. Plaintiff is, and at all times relevant hereto was, a citizen and resident of San Luis Obispo County, California.

8. Plaintiff is, and at all times relevant hereto was, a user of Meta.

9. Plaintiff is a consumer of the video products and services offered on Defendant's www.nationalnotary.org website. Including on or about August 2024, Plaintiff purchased prerecorded video material from Defendant's www.nationalnotary.org website by requesting and paying for such material, providing her name, email address, and home address for delivery of such material. Defendant completed the sales of goods to Plaintiff by shipping or delivering the prerecorded video material she purchased to the address she provided in her order. Accordingly, Plaintiff requested or obtained, and is therefore a consumer of, prerecorded video material sold by Defendant on its website.

10. At all times relevant hereto, including when requesting or obtaining prerecorded video material from Defendant's website, Plaintiff had a Meta account, a Meta profile displaying her name and picture, and an FID associated with such profile.

11. Plaintiff has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her Private Video Information to Meta. In fact, Defendant has never even provided Plaintiff with written notice of its practices of disclosing its customers' Private Video Information to third parties such as Meta.

12. Prior to and at the time she purchased prerecorded video material from Defendant, Defendant did not notify Plaintiff that it would disclose the Private Video Information of its customers generally or that of Plaintiff in particular, and Plaintiff has never consented, agreed, authorized, or otherwise permitted Defendant to disclose her

Private Video Information to third parties. Plaintiff has never been provided any written notice that Defendant discloses its customers' Private Video Information or any means of opting out of such disclosures of her Private Video Information.

13. Because Defendant disclosed Plaintiff's Private Video Information (including her FID, unique identifiers, and her request or purchase of prerecorded video material from Defendant's website) to third parties during the applicable statutory period, Defendant violated Plaintiff's rights under the VPPA and invaded her statutorily conferred interest in keeping such information (which bears on her personal affairs and concerns) private.

II. Defendant

14. Defendant National Notary Association is a not-for-profit corporation organized under the laws of California, with its headquarters at 9350 De Soto Ave., Chatsworth, California 91311. Defendant is the largest and oldest organization in the United States serving notaries and training persons to be notaries through certifications, trainings, seminars, conferences, and printed and online educational materials that accompany these programs.

C. JURISDICTION AND VENUE

15. The Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

16. Personal jurisdiction and venue are proper because Defendant maintains its headquarters and principal place of business in Los Angeles, California, within this judicial District.

VIDEO PRIVACY PROTECTION ACT

17. The VPPA prohibits companies (like Defendant) from knowingly disclosing to third parties (like Meta) information that personally identifies consumers (like Plaintiff) as having requested or obtained specific video(s) or other audio-visual materials from its Website.

18. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," 18 U.S.C. § 2710(a)(4). It defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3).

19. Leading up to the VPPA's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

20. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, the personal nature of such information, and the need to protect it from disclosure, is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id.*

21. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a more recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[1]

22. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[2]

23. In this case, however, Defendant deprived Plaintiff and numerous other similarly situated persons of that right by systematically (and surreptitiously)

---

[1] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary. senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the- 21stcentury.

[2] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, franken.senate.gov (Jan. 31, 2012).

disclosing their Private Video Information to Meta, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

24. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[3]

25. Over two decades later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a 26 billion dollar per year online advertising industry in the United States.[4]

26. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

[3] Transcript, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[4] *See* Julia Angwin and Emily Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), available at https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[5]

27. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[6]

28. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[7]

---

[5] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

[6] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), available at http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/ .

[7] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), available at https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html#:~:text=It's%20called%20the%20Acxiom%20Corporation,to%20know%20much%2C%20much%20more.

29. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[8]

30. Recognizing the severe threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[9]

31. Data aggregation is especially troublesome when consumer information is sold to direct-mail advertisers. In addition to causing waste and inconvenience, direct-mail advertisers often use consumer information to lure unsuspecting consumers

---

[8] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. On Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) available at https://www.commerce.senate.gov/services/files/3bb94703-5ac8-4157-a97b-%20a658c3c3061c.

[9] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012), available at https://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

into various scams, including fraudulent sweepstakes, charities, and buying clubs. Thus, when companies like Defendant share information with data aggregators, data cooperatives, and direct-mail advertisers, they contribute to the "[v]ast databases" of consumer data that are often "sold to thieves by large publicly traded companies," which "put[s] almost anyone within the reach of fraudulent telemarketers" and other criminals.[10]

32. Disclosures like Defendant's are particularly dangerous to the elderly. "Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide."[11]

33. The FTC notes that "[t]he elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers."[12]

34. Indeed, an entire black market exists while the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like

---

[10] *See* Charles Duhigg, *Bilking the Elderly, with a Corporate Assist*, N.Y. Times (May 20, 2007), available at https://www.nytimes.com/2007/05/20/business/20tele.html.

[11] *Id*.

[12] Prepared Statement of the FTC on "Fraud Against Seniors" before the Special Committee on Aging, United States Senate (August 10, 2000).

Defendant's are particularly troublesome because of their cascading nature: "Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[13]

35. Defendant is not alone in violating its customers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

II. Consumers Place Monetary Value on Their Privacy and Consider Privacy Practices When Making Purchases

36. As the data aggregation industry has grown, so has consumer concerns regarding personal information.

37. A survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do protect their privacy online.[14] As a result, 81 percent of smartphone

---

[13] *Id*.

[14] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[15]

38. Thus, as consumer privacy concerns grow, consumers increasingly incorporate privacy concerns and values into their purchasing decisions, and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy-protective competitors. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[16]

39. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[17]

---

[15] *Id*.

[16] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), available at https://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

[17] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on Monetizing Privacy*

40. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[18] As such, where a business offers customers a product or service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a product or service of less value than the product or service paid for.

III. Defendant Use the Meta Pixel to Systematically Disclose its customers' Private Video Information to Meta

41. As alleged below, when a consumer requests or obtains a particular prerecorded video on Defendant's Website, the Meta Pixel technology that Defendant intentionally installed on its Website transmits (1) the unencrypted FID for each purchaser; (2) detailed information revealing the titles and subject matter of the prerecorded videos requested or obtained by each of its purchasers; and (3) the URL where such videos are available for purchase, without the consumer's consent and in clear violation of the VPPA.

(Feb. 27, 2012), available at https://www.enisa.europa.eu/publications/monetising-privacy.

[18] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf.

A. The Meta Pixel

42. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta".[19] Meta is now the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birth date, gender, and phone number or email address.

43. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to monitor and track the actions taken by visitors to their websites and to report them back to Meta. This allows companies like Defendant to build detailed profiles about its customers and to serve them with highly targeted advertising.

44. Additionally, the Meta Pixel installed on a company's website allows Meta to "match [] website visitors to their respective Facebook User accounts."[20] This is because Meta has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name[21] – and because each transmission of information made

[19] *See* Facebook, "Company Info," available at https://about.fb.com/company-info./.

[20] Meta, "Get Started – Meta Pixel," available at https://developers.facebook.com/docs/meta-pixel/get-started/.

[21] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark

from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor.

45. As Meta's developer's guide explains, installing the Meta Pixel on a website allows Meta to track actions that users with Meta accounts take on the site. Meta states that "Examples of [these] actions include adding an item to their shopping cart or making a purchase."[22]

46. Meta's Business Tools Terms govern the use of Meta's Business Tools, including the Meta Pixel.[23]

47. Meta's Business Tools Terms state that website operators may use Meta's Business Tools, including the Meta Pixel, to transmit the "Contact Information" and "Event Data" of their website's visitors to Meta.

48. Meta's Business Tools Terms define "Contact Information" as "information that personally identifies individuals, such as names, email addresses, and phone numbers . . . ."[24]

Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

[22] Meta, "About Meta Pixel," available at https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[23] Meta, "Meta Business Tools Terms," available at https://www.facebook.com/legal/technology_terms.

[24] *Id.*

49. Meta's Business Tools Terms state: "You instruct us to process the Contact Information solely to match the Contact Information against user IDs [e.g., FIDs] ("Matched User IDs"), as well as to combine those user IDs with corresponding Event Data."[25]

50. The Business Tools Terms define "Event Data" as, *inter alia*, "information that you share about people and the actions that they take on your websites and apps or in your shops, such as visits to your sites, installations of your apps, and purchases of your products."[26]

51. Website operators use the Meta Pixel to send information about visitors to their Websites to Meta. Every transmission to Meta accomplished through the Meta Pixel includes at least two elements: (1) the website visitor's FID and (2) the webpage's URL triggering the transmission.

52. Depending on the configuration of the Meta Pixel, the website may also send Event Data to Meta. Defendant have configured the Meta Pixel on its Website to send Event Data to Meta.

[25] *Id.*

[26] *Id.*

53. When website operators make transmissions to Meta through the Meta Pixel, none of the following categories of information are hashed or encrypted: the visitor's FID, the website URL, or the Event Data.

54. Every website operator installing the Meta Pixel must agree to the Meta Business Tools Terms.[27]

55. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after the consumer's browser history has been cleared.

56. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

57. Simply put, if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it

[27] *See id.*

transmits) are then able to "track [] the people and type of actions they take,"[28] including, as relevant here, the specific prerecorded video material that they purchase from Defendant's website.

B. Defendant Knowingly Uses the Meta Pixel to Transmit the Private Video Information of its Customers to Meta

58. Defendant sells various prerecorded video materials on its Website, www.nationalnotary.org, including online courses and certification programs on various topics, including becoming a licensed notary or signing agent.

59. To purchase prerecorded video material from both Defendant's Website, a person must provide at least his or her name, email address, billing address, and credit or debit card (or other form of payment) information.

60. During the purchase process on Defendant's Website, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the person who made the purchase and the specific title of video material that the person purchased (as well as the URL where such video material is available for purchase).

[28] Meta, "Retargeting: How to Advertise to Existing Customers with Ads on Facebook," available at https://www.facebook.com/business/goals/retargeting?checkpoint_src=any.

61. In order to take advantage of the targeted advertising and other informational and analytical services offered by Meta, Defendant intentionally programmed its Website (by following step-by-step instructions from Meta's website) to include the Meta Pixel code, which systematically transmits to Meta the FID of each person with a Meta account who purchases prerecorded video material on Defendant's Website, along with the specific title of the prerecorded video material that the person purchased.

62. With only a person's FID and the title of the prerecorded video material (or URL where such material is available for purchase) that the person purchased from Defendant's Website —all of which Defendant knowingly and systematically provides to Meta—any ordinary person could learn the identity of the person to whom the FID corresponds and the subscription or the title of the specific prerecorded video material that the person purchased (and thus requested and obtained). This can be accomplished simply by accessing the URL www.facebook.com/ and inserting the person's FID.

63. Defendant's practice of disclosing the Private Video Information of its customers to Meta continued unabated for the duration of the two-year period preceding the filing of this action. At all times relevant hereto, whenever Plaintiff or any other person purchased prerecorded video material from Defendant on its Website, Defendant disclosed to Meta (*inter alia*) the specific title of the video material that was requested or obtained (including the URL where such material is available for

purchase), along with the FID of the person who requested or obtained it (which, as discussed above, uniquely identified the person).

64. At all times relevant hereto, Defendant knew the Meta Pixel was disclosing its customers' Private Video Information to Meta.

65. Although Defendant could easily have programmed its Website so that none of its customers' Private Video Information is disclosed to Meta, Defendant instead chose to program its Website so that all of its customers' Private Video Information is disclosed to Meta.

66. Before transmitting its customers' Private Video Information to Meta, Defendant failed to notify any of them that it would do so, and none of them have ever consented (in writing or otherwise) to these practices.

67. By intentionally disclosing to Meta Plaintiff's and their other customers' FIDs together with the specific title of the prerecorded video material that they each purchased, without any of their consent to these practices, Defendant knowingly violated the VPPA on an enormous scale.

CLASS ACTION ALLEGATIONS

68. Plaintiff seeks to represent a class defined as all persons in the United States who, during the two years preceding the filing of this action, purchased prerecorded video material or services from Defendant's Website while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

69. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the Defendant's membership records.

70. Common questions of law and fact exist for all Class members and predominate over questions affecting only individual class members. Common legal and factual questions include but are not limited to (a) whether Defendant embedded Meta Pixel on its Website that monitors and tracks actions taken by visitors to its Website; (b) whether Defendant reports the actions and information of visitors to Meta; (c) whether Defendant knowingly disclosed Plaintiff's and Class members' Private Video Information to Meta; (d) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; and (e) whether Plaintiff and Class members are entitled to a statutory damage award of $2,500, as provided by the VPPA.

71. The named Plaintiff's claims are typical of the claims of the Class in that the Defendant's conduct toward the putative class is the same. That is, Defendant embedded the Meta Pixel on its Website to monitor and track actions taken by consumers on its Website and report this to Meta. Further, the named Plaintiff and the Class members suffered invasions of their statutorily protected right to privacy (as

afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Private Purchase Information to Meta.

72. Plaintiff is an adequate representative of the Class because she is interested in the litigation; her interests do not conflict with those of the Class members she seeks to represent; she has retained competent counsel experienced in prosecuting class actions; and she intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of all Class members.

73. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication of the common questions of law and fact, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability

issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION
Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710

74. Plaintiff repeats the allegations asserted in the preceding paragraphs as if fully set forth herein.

75. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

76. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant are each a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because they engaged in the business of selling and delivering prerecorded video materials, similar to prerecorded video cassette tapes, to consumers nationwide.

77. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiff and Class members are each a "consumer" within the meaning

of the VPPA because they each purchased prerecorded video material or services from Defendant's Website that were sold and delivered to them by Defendant.

78. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The Private Video Information that Defendant transmitted to Meta constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because it identified Plaintiff and Class members to Meta as an individual who "requested or obtained," specific prerecorded video material from Defendant's Website.

79. Defendant knowingly disclosed Plaintiff's and Class members' Private Video Information to Meta via the Meta Pixel technology because Defendant intentionally installed and programmed the Meta Pixel code on its Website, knowing that such code would transmit the prerecorded video material requested or obtained by their consumers and the consumers' unique identifiers (including FIDs).

80. Defendant failed to obtain informed written consent from Plaintiff or Class members authorizing Defendant to disclose their Private Video Information to Meta or any other third party. More specifically, at no time prior to or during the applicable statutory period did Defendant obtain from any person who requested or obtained prerecorded video material or services on Defendant's Website (including Plaintiff or Class members) informed, written consent that was given in a form distinct

and separate from any form setting forth other legal or financial obligations of the consumer, that was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner, or that was given after Defendant provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

81. By disclosing Plaintiff's and Class members' Private Video Information, Defendant violated their statutorily protected right to privacy in their Private Video Information.

82. Consequently, Defendant is liable to Plaintiff and Class members for damages in the statutorily set sum of $2,500. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendant as follows:

a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as the representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b) For an order declaring that Defendant's conduct as described herein violated the VPPA;

c) For an order finding in favor of Plaintiff and the Class and against Defendant on all counts asserted herein;

d) For an award of $2,500.00 to Plaintiff and each Class member, as provided by 18 U.S.C. § 2710(c);

e) For an order permanently enjoining Defendant from disclosing the Private Video Information of its subscribers to third parties in violation of the VPPA;

f) For prejudgment interest on all amounts awarded; and

g) For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiff and the Class under Rule 23 and 18 U.S.C. § 2710(c).

Dated: January 13, 2025

Respectfully submitted,

HEDIN LLP

By: /s/ *Frank S. Hedin*

FRANK S. HEDIN (SBN 291289)
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Counsel for Plaintiff and the Putative Class